UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/611,254	07/01/2003	Pierre-Yvan Liardet	S01022.81054.US	1137

23628 7590 05/31/2007

WOLF GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

MAIL DATE	DELIVERY MODE
05/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/611,254	LIARDET ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 May 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The request filed on May 11, 2007 for a request for continued examination (RCE) under 37 CFR 1.114 based on patent application 10/611,254 is acceptable and an RCE has been established.

2. All independent claims, namely claims **1, 8 and 10** are amended. Three new dependent claims, namely claims 15-17 have been added. Thus, claims 1-17 are pending.

Response to Arguments

3. Applicant's remark/arguments filed on May 11, 2007 have been fully considered but they are not persuasive.

Applicant's representative added the following limitation in each and every independent claim and argued that the added limitation is neither disclosed by the admitted prior art nor by the reference on the record, namely view Snell.

"**wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical**."

Examiner disagrees with the above argument.

Examiner would like to point out that the limitation does not have support in the specification. Note that the only support the specification contains is that "first random number having the size of said code and all the blocks of each have the same value" and this is different from the limitation "**wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical".** For the sake of examination, Examiner interprets such limitation as "first random number having the size of said code and all the blocks of each have the same value"

In order to show how each and every limitation of at least the independent claims are disclosed by the reference on the record, the examiner would show the following.

Admission discloses a cyphering/decyphering method [page 1, lines 17-18] (AES "Advanced Encryption Standard, "cyphering/deciphering") by **an integrated circuit,** [page 3, line 21] (implementation on smart cards of AES-type algorithms) **of a digital input code (S_0, S_n)** [page 1, lines 25-26] **by means of several keys (K_i),**[page 1, lines 20-21] ("different ciphering keys") **consisting of**:

- **Dividing said code into several data blocks of same dimensions;** [page 1, lines 19-21 and page 1, lines 27-28] (On page 1, lines 19-21, it has been recited that the code is divided and on page 1, lines 27-28, it is disclosed that that each block has the same size) and

- **Applying to said blocks multiple turns (T) of a cyphering or decyphering consisting of submitting each block to at least one same non-linear transformation (SUBBYTES, INVSUBBYTES)** [page 2, lines 12-29 and figure 3, ref. Num "4" and figure 4, ref. Num "24"] **and of subsequently combining each block with a different key (Ki) at each turn, [**page 2, lines 12-14 and page 1, lines 20-21**] and**

- **Masking the inputs and outputs of the non-linear transformation, upon execution of the method, by means of at least one first random number (R1)** [page 4, lines 2-6; page 4, lines 7-19 and page 5, lines 7-11] **having the size of said code and all the blocks of which have the same value by combining, by an XOR-type function, the input and output blocks of the non-linear transformation with said random number.** [Page 4, lines 2-

6; page 4, lines 7-19 and page 5, lines 7-11 and figure 3, ref. Num "12", ref. Num, "13" and figure 4, ref. Num "22" and ref. Num "23" & figure 4 and 5]

- Admission does not explicitly teach the following new limitation which is added into the respective independent claims "**wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical**" and this limitation which is found to be a new matter is interpreted as "that the random number (R1) and the code having the size."

However, in the field of endeavor **Snell**, discloses

- The circuit wherein the pseudo-random generator and XOR array of the dummy circuit **having a word width in bits identical** to that of pre-mix subcircuit in the which it is configured to perform AES or Advanced Encryption standard. [Abstract; claim 1 and 7]

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. **Claims 1-17** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The independent claim(s) namely claims 1, 8 and 10 contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Based on a thorough review of the entire disclosure and a text search for the

limitation "**wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical**", there is no "readily apparent support" how the first random number is comprising of a plurality of blocks of bits and how these blocks of bits are identical.

Therefore the examiner does not find support in the specification for the amended limitation in particular to the limitation "**wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical**" and found this limitation as a new matters.

As it is mentioned above, for the sake of examination examiner interprets such limitation as "first random number having the size of said code and all the blocks of each have the same value." Note such interpretation is given since this the only thing disclosed in the entire specification that is close to the new matter introduced in the amended claims.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1-17** are rejected under 35 U.S.C. 103(a) as being unpatentable over admitted prior art (hereinafter referred to as **Admission**) in view Snell (hereinafter referred to as **Snell**) (US Publication No. 2003/0223580 A1) (claims priority of provisional application No. 60/383,252 filed on 05/23/2002)

8. **As per claims 1, 3, 8, 10 and 15-17, Admission discloses a cyphering/decyphering method** [page 1, lines 17-18] (AES "Advanced Encryption Standard, "cyphering/deciphering") by **an integrated circuit,** [page 3, line 21] (implementation on smart cards of AES-type algorithms) **of a digital input code (S_0, S_n)** [page 1, lines 25-26] **by means of several keys (K_i),**[page 1, lines 20-21] ("different ciphering keys") **consisting of**:

- **Dividing said code into several data blocks of same dimensions;** [page 1, lines 19-21 and page 1, lines 27-28] (On page 1, lines 19-21, it has been recited that the code is divided and on page 1, lines 27-28, it is disclosed that that each block has the same size) and

- **Applying to said blocks multiple turns (T) of a cyphering or decyphering consisting of submitting each block to at least one same non-linear transformation (SUBBYTES, INVSUBBYTES)** [page 2, lines 12-29 and figure 3, ref. Num "4" and figure 4, ref. Num "24"] **and of subsequently combining each block with a different key (Ki) at each turn, [**page 2, lines 12-14 and page 1, lines 20-21**] and**

- **Masking the inputs and outputs of the non-linear transformation, upon execution of the method, by means of at least one first random number (R1)** [page 4, lines 2-6; page 4, lines 7-19 and page 5, lines 7-11] **having the size of said code and all the blocks of which have the same value by combining, by an XOR-type function, the input and output blocks of the non-linear transformation with said random number.** [Page 4, lines 2-6; page 4, lines 7-19 and page 5, lines 7-11 and figure 3, ref. Num "12", ref. Num, "13" and figure 4, ref. Num "22" and ref. Num "23" & figure 4 and 5]

- Admission does not explicitly teach the following new limitation which is added into the respective independent claims "**wherein the at least one first random number comprises a plurality of blocks of bits and wherein each block of bits is identical**" and this limitation which is found to be a new matter is interpreted as "that the random number (R1) and the code having the size."

However, in the field of endeavor **Snell**, discloses

- The circuit wherein the pseudo-random generator and XOR array of the dummy circuit **having a word width in bits identical** to that of pre-mix subcircuit in the which it is configured to perform AES or Advanced Encryption standard. [Abstract; claim 1 and 7]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to add the features of the circuit wherein the pseudo-random generator and XOR array of the dummy circuit having a word width in bits identical to that of pre-mix subcircuit in the which, it is configured to perform AES or Advanced Encryption standard as per teachings of **Snell** in to the method as taught by **Admission**, in order to counteract differential power analysis attacks in symmetric key block cipher algorithm such AES/Rijndael. [See, **Snell**, Paragraph 0002]

9. **As per claim 2**, the combination of **Admission and Snell** discloses the method as applied to claims above. Furthermore, Admission discloses the method, consisting of combining the input code (S_0, S_n) with a second random number (R) of same dimension as the code. [page 5, lines 7-11, figure 4, ref. Num "23" RD2]

10. **As per claims 4 and 14**, the combination of **Admission and Snell** discloses the method as applied to claims above. Furthermore, Admission discloses the

method wherein, any of claims 1 to 3, applied to an AES-type cyphering algorithm. [page 1, lines 17-24, figure 1-4]

11. **As per claims 5-7 and 11-13**, the combination of Admission and Snell discloses the method as applied to claims above. Furthermore, Admission discloses the method, wherein said first random number (R1) is changed at each cyphering turn. [Figure 3, figure 4, page 4, lines 7-19; page 5, lines 7-8, figure 4, ref. Num "22 & 23" RD1 & RD2] (Since at each turn, the key changes so does the random number)

12. **As per claim 9**, the combination of Admission and Snell discloses the method as applied to claims above. Furthermore, Admission discloses the method, comprising means for implementing the method of any of claims 1 to 7. [figure 3 & figure 4]

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private

PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
05/25/2007

Examiner AU 2132